



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,013	07/26/2001	Charlie Udom	10011169-1	9668

7590 03/07/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/917,013

Applicant(s)

UDOM, CHARLIE

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 July 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>07062004</u> . | 6) <input type="checkbox"/> Other: _____ |

Drawings

10 ***Claim Rejections - 35 USC § 112***

Claim Rejections - 35 USC § 102

30 Claims 1-18 and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Catalano, U.S. Patent No. 6,766,040.

Art Unit: 2137

As per claims 1,8,9,10, and 14, the applicant describes a biometric security device comprising the following limitations:

a) a biometric scanner having an output data port (Col 2, lines 27-30);

5 b) a processor having an input data port coupled to said data output port of said biometric scanner and further having an output data port (Col 2, lines 30-41; Col 4, line26-28);

c) a data transmitter having an input port coupled to the output port of said processor device (Col 5, lines 47-55);

10 The security device can best be viewed in regards to figure 1 which illustrates a biometric scanner for obtaining a first biometric characteristic in 130 (part a), memory for storing a second biometric characteristic in 120, a processor, coupled to the scanner and the memory, in 110 (part b), and a data transmitter, coupled to the processor, in 150. The data transmitter, or interface transmits a signal indicating that a person has been identified.

15 Regarding claim 10, the fingerprint identification security device that Catalano discloses is described as being built upon a "PDA, cellular telephone, or other portable device" (Col 1, line 62-63), so the use of a PDA providing the processing means is disclosed.

Regarding claim 14, the use of a capacitive finger-print scanner is disclosed (Col 5, lines 13-14) as is the use of memory (Col 2, lines 30-35).

20 As per claim 2, the applicant describes the biometric security device of claim 1, which is met by Catalano (see above), with the following limitation which is also anticipated by Catalano:

Wherein said biometric scanner is a finger print scanner (Col 5, line 1).

25 As per claim 3, the applicant describes the biometric security device of claim 1, which is met by Catalano (see above), with the following limitation which is also anticipated by Catalano:

Art Unit: 2137

Further including a memory coupled to said processor and having stored therein at least one of:
an identifier for said biometric security device and data representing a biometric characteristic of at least
one individual (Col 2, lines 30-35).

5 As per claims 4,5, and 13, the applicant describes the biometric security device of claims 1,3, and
10, which are met by Catalano (see above), with the following limitation which is also anticipated by
Catalano:

Wherein said biometric data transmitter is a Bluetooth protocol-compliant transmitter (Col 5, lines
46-55).

10 As per claim 6, the applicant describes the biometric security device of claim 1, which is met by
Catalano (see above), with the following limitation which is also met by Catalano:

Wherein said processor is a personal digital assistant (Col 1, lines 59-64).

15 As per claims 7 and 16, the applicant describes the biometric security device of claims 1 and 14,
which are met by Catalano (see above), with the following limitation which is also met by Catalano:

Wherein said biometric data transmitter is an infrared transmitter (Col 5, lines 46-55).

20 As per claim 11, the applicant describes the biometric security device of claim 10, which is met by
Catalano (see above), with the following limitation which is also anticipated by Catalano:

Further including a memory coupled to said processor which stores an authenticator for said
personal digital assistant (Col 2, lines 32-38);

The stored user traits are authenticators for the PDA to authenticate an incoming fingerprint with
a stored fingerprint.

25 As per claim 12, the applicant describes the biometric security device of claim 10, which is met by
Catalano (see above), with the following limitation which is also anticipated by Catalano:

Art Unit: 2137

Wherein said image scanner is a capacitive finger scanner (Col 5, lines 13-14).

As per claim 15, the applicant describes the biometric security device of claim 14, which is met by Catalano (see above), with the following limitation which is also anticipated by Catalano:

5 Wherein said capacitive finger-print scanner is a fingerprint scanner that generates a numerical representation of a finger-print of an individual (Col 5, lines 13-18; Col 9, line 64 to Col 10, line 12).

As per claims 17, the applicant describes the limitations of the biometric security device of claim 1, which is met by Catalano (see above), with the additional limitation of a retinal image scanner instead
10 of a fingerprint scanner which is met by Catalano (Col 18, lines 40-51).

As per claim 18, the applicant describes the limitations of the biometric security device of claim 1 with the retinal image scanner of claim 17, which is met by Catalano (see above), with the additional limitation that the retinal image scanner has an output port which connects the scanner to the processor
15 and the processor has an output port which connects the processor to the transmitter. This limitation is met by Fig 1 of Catalano in which the fingerprint sensor is replaced by the retinal sensor (Col 18, lines 40-51), the logic unit is a processor (Col 4, lines 15-17), and the interface is a transmitter (Col 5, lines 47-55).

As per claim 24, the applicant describes a biometric security device comprising the following
20 limitations which are met by Catalano:

a) a capacitive finger print image scanner obtaining a first biometric characteristic (Col 5, lines 13-14);

b) a personal digital assistant device having a processor coupled to said capacitive finger print image scanner (Col 2, lines 30-38; Col 1, lines 59-63);

25 c) a memory coupled to said processor and storing at least one of a second biometric characteristic and an identifier for said biometric security device (Col 2, lines 32-38);

Art Unit: 2137

d) a Bluetooth communication protocol-compliant data transmitter coupled to said processor and capable of transmitting at least one of said identifier, said first biometric characteristic, and a signal representing the results of comparing said first biometric characteristic to said second biometric characteristic (Col 5, lines 47-55).

5

Claims 19-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Bjorn, U.S. Patent No. 6,741,729.

As per claim 19, the applicant describes a method of controlling access to an area using a biometric characteristic of individuals comprised of the following limitations which are met by Bjorn:

- a) scanning a biometric characteristic of an individual (Col 4, lines 25-27);
- b) generating a numeric representation of said biometric characteristic (Col 4, lines 1-5);
- c) modulating said numeric representation onto a radio frequency (RF) signal (Col 4, lines 20-24);
- d) transmitting said RF signal to a radio receiver for analysis (Col 4, lines 20-24).

15 Bjorn describes a system similar to that of the applicant's and that of Catalano as cited above with the difference that Bjorn discloses the comparison of the scanned biometric characteristic taking place at the remote location. Also, instead of sending a yes/no response for access from the sensor device as in Catalano above, Bjorn discloses digitizing the biometric characteristic into a numeric representation and transmitting the digitized numeric representation through one of a variety of

20 transmission means, including through radio frequency signals.

As per claim 20, the applicant describes a method of controlling access to an area using biometric characteristics of individuals comprising the following limitations which are met by Bjorn:

- a) obtaining a first biometric characteristic of an individual (Col 8, lines 32-33);
- 25 b) generating a first numeric representation of said first biometric characteristic (Col 5, lines 37-41);

Art Unit: 2137

c) comparing said first numeric representation to a second numeric representation of a biometric characteristic of an individual authorized to have access to said area (Col 8, line 54 to Col 9, line 13);

d) upon the determination that said first numeric representation is at least substantially the same as said second numeric representation, modulating said first numeric representation onto a radio

5 frequency (RF) signal (Col 8, line 54 to Col 9, line 13; Col 4, lines 20-24);

e) transmitting said RF signal to a radio receiver for analysis (Col 8, line 54 to Col 9, line 13; Col 4, line 20-24);

Bjorn discloses that comparison of the scanned image can take place on both the digital system (110 of Fig 1) and the scanner (150 of Fig 1) in such cases as when the digital system may not be secure.

10 Thus, parts a) and b) above take place on the scanner. Parts c),d), and e) take place on the digital system. If a match occurs on the preliminary comparison of the digital system, it is transmitted back to the scanner so that the scanner can make the final decision. The communication can be RF signaling (Col 4, lines 20-24) which would involve modulating the digital representation of the fingerprint in order to send it back to the scanner for final analysis. The radio receiver in part e) is the scanner.

15

As per claims 21 and 23, the applicant describes the method of claims 20 and 22, which are met by Bjorn (see above), with the following limitation which is also met by Bjorn:

Wherein said step of obtaining a first biometric characteristic is comprised of the step of optically scanning a first biometric characteristic (Col 6, lines 67 to Col 7, line 2).

20

As per claim 22, the applicant describes a method of controlling access to an area using biometric characteristics of individuals comprising the following limitations:

a) obtaining a first biometric characteristic of an individual (Col 4, lines 25-27);

b) generating a first numeric representation of said first biometric characteristic (Col 4, lines 1-5);

25 c) modulating said first numeric representation onto a radio frequency (RF) signal (Col 4, lines 20-24);

d) transmitting said RF signal to a radio receiver for demodulation (Col 4, lines 20-24);

Art Unit: 2137

e) after demodulating said RF signal, comparing said first numeric representation to a second numeric representation of a biometric characteristic of an individual authorized to have access to said area (Col 4, lines 1-5);

f) upon the determination that said first numeric representation is at least substantially the same as said second numeric representation, enabling access to said area (Col 15, line 65- Col 16, line 11);

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

10 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15 Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Catalano in view of Bjorn.

20 As per claim 11, the applicant describes the biometric security device of claim 10, which is met by Catalano (see above), with the following additional limitation which is met by Bjorn:

Further including a memory coupled to said processor which stores an authenticator for said personal digital assistant (Bjorn: Col 9, lines 42-52);

25 Claim 11 has already been rejected under 35 U.S.C. 102(e) because the claim is broad enough for an authenticator to represent a user trait stored in the PDA which authenticates a scanned fingerprint. The intended meaning of the claim is to provide the limitation that the PDA is authenticated when it transmits a signal to the remote location. This is accomplished by Bjorn through the use of public/private key cryptography.

30 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Bjorn with those of Catalano and add the use of public/private key cryptography

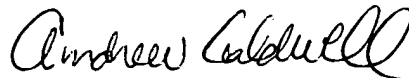
Art Unit: 2137

into the transmitted signal from the sensor/PDA device to the remote device so that the remote device can authenticate the sensor/PDA device.

5 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

 If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where
10 this application or proceeding is assigned is 703-872-9306.

 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
15 you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER